

In May and June 2021 Flashbots strengthened and moved forward our network, successfully releasing v0.2 and with it improved auction pricing as well as bundle merging.

Overview

At the time of writing mining pools accounting for more than 84% of the Ethereum network hashrate have adopted Flashbots and more searchers than ever are submitting and landing bundles on-chain. More metrics on Flashbots and its stakeholders can be found on our [Transparency Dashboard](#).

As an open research organization we stayed true to our commitment to learning from the community and iterating in public. Here are the highlights:

- [Released Flashbots Auction v0.2 and bundle merging](#) (May 24th)
- [Released ethresearch post: MEV-SGX Proposal](#) (May 31st)
- [Released research post: MEV in ETH2 — an early exploration](#) (June 10th)

Flashbots Auction

Released v0.2

In early April we published our initial proposal for Flashbots Auction v0.2 to gather feedback and share our roadmap. We released v0.2 on May 24th with these features: * *Bundle merging (full-release)*: More revenue for miners, higher chance of inclusion for searchers.

- *New geth config introducing strict profit switching (optional, full-release)*: Eliminates empty block race condition (i.e. mining 2 gwei transaction), but increases latency hence may impact profitability.

We ultimately decided to remove the following features:

- *Proxy payment contract*: this feature was originally designed to enable better logging and to enable future solutions that attempted to prevent time bandit attacks. It was removed after receiving feedback from the searcher community that the proxy payment contract would add additional costs without providing finality guarantees.
- *Full block submission*: this feature was removed from the v0.2 release in order to reduce the complexity of the release.
- *Replace HTTP endpoints with WebSockets (full-release)*: this feature was removed to reduce complexity of v0.2

Release v0.2.2

In early June we discovered that some searchers were gaming the Flashbots auction and underpaying miners for inclusion. The heart of the bug was that MEV-Geth did not ensure that the gas price that bundles paid post-merging was the same as what we thought it was pre-merge. Since bundles are simulated alone at the head of a block, if a bundle could somehow change the amount it paid based on their position in a block then that bundle could trick MEV-Geth if it was merged in the 2nd or later bundle position.

Given that this affected both searcher and miner's profitability we pushed a fix in release v0.2.2 to this. The fix for this issue can be found [here](#).

Release v0.2.3

As part of the update to bundle scoring in release v0.2 we started to discount the fees from transactions that had been seen in the mempool in order to prevent "bundle stuffing," where searchers take high gas price transactions from the mempool and include them in their bundles in order to "piggyback" off of those gas prices and get some transactions accepted that otherwise wouldn't have been.

Our implementation of this discounting did fix bundle stuffing, but it also wrongly penalized a class of searchers who submit both transactions in the regular mempool and Flashbots transactions at the same time. Essentially we wrongly discounted coinbase payments from these transactions, which meant they landed in Flashbots blocks much less often than they should. The fix for this issue can be found [here](#).

Bundle merging highlights

Since bundle merging launched we can see a substantial increase in the number of bundles included in blocks. In fact the number of bundles more than doubled, going from ~6,000 to ~13,000 in the weeks after bundle merging was launched.

□

Bundle merging saw strong and consistent adoption, reaching nearly ~70% of Flashbots blocks having 2 or more bundles included in them

□

In turn the amount of MEV that miners make per block has increased relative to normal transaction fees. The chart below shows average MEV profit divided by transaction fees, measured on a daily basis. This demonstrates that while the overall profitability of Flashbots blocks has been decreasing, that drop can be attributed to the decrease in gas prices recently and Flashbots is actually accounting for an increasing amount of miner's revenue over time.

□

EIP1559

With the London fork around the corner, the Flashbots team has shifted focus towards adding support for EIP-1559 to MEV-Geth and Flashbots Relay. Flashbots aims to have MEV-Geth v0.3 released at the end of June to support the Goerli upgrade to EIP-1559 on block 5062605: <https://blog.ethereum.org/2021/06/18/london-testnets-announcement/>

EIP-1559 has big implications for searchers and miners. Searchers will need to adapt their bots to use a new transaction format and will be required to pay the `base_fee` for each of their transactions. This means it is no longer possible to achieve "0 gas" transactions. We are hoping to introduce upgrades to ethereum and flashbots in the future which re-enable this behavior. On the miner's side, EIP-1559 will have an impact on their accounting and node infrastructure. We expect EIP-1559 to further increase miner's desire to receive value from MEV.

Flashbots Research is currently analyzing the impact of EIP-1559 on MEV and Flashbots. The preliminary results will be presented in MEV.wtf summit on Jul 1, followed by a research post.

Reputation

We are starting to experiment with a reputation system to handle the load we have been receiving in periods of heavy activity — this should lead to improved relay performance for searchers with a history of successful inclusions. While we expect this change to have an immediate positive impact, it is a temporary solution and we are actively looking for feedback on how we should think about scaling the relay moving forward. See our proposal here: <https://github.com/flashbots/pm/discussions/79>

Flashbots Data

New monitoring tools

Working with our community contributor [@metachris](#) we've developed a series of monitoring tools that enable us to better understand implementations of Flashbots' network, miners behaviour, and any deviations in the expected behaviour of the Flashbots blockspace auction. Specifically we have tools to monitor [reverted 0 gas price transactions](#) and when bundles are not ordered according to their effective gas price. We intend to productionize these monitoring tools and create a Discord channel that provides alerts from them.

Transparency Dashboard

As a reminder we maintain a dashboard on the Flashbots network [here](#). It was designed to give the community transparency on the Flashbots Network and contains a collection of real time metrics on Flashbots and its stakeholders. We highly recommend looking through the Flashbots Transparency Dashboard.

Flashbots Research

MEV-SGX

Flashbots Alpha has been and continues to be successful, but it offers incomplete trust guarantees. In particular it is not *permissionless* nor is it *completely private*. These are extremely difficult properties to achieve. In our pursuit of these properties Flashbots has released our proposal, MEV-SGX, for using secure enclaves to provide a permissionlessness and complete privacy. Read more about the MEV-SGX [here](#).

MEV in eth2

As The Merge approaches, we've begun research efforts in understanding MEV in eth2 better. Our first research post on the

topic was released [here](#), alongside a [repository](#) with some rough modeling of staking rewards with MEV. In this early exploration, we study transaction ordering in eth2 and analyze MEV-enabled staking yields. We find that MEV will significantly boost validator rewards but may reinforce inequalities within participants of eth2. We also discuss qualitative aspects of MEV in eth2 such as the potential dynamics that will unfold between its largest stakeholders like exchanges and validator pools.

This follows our joint prototyping experiment with Nethermind and Lido in ETHGlobal [Ray Tracing](#).

Ongoing research efforts:

There are multiple ongoing research efforts worked on by Flashbots team members, external collaborators and MEV Fellows. Learn more about Flashbots Research [here](#).

- MEV in eth2 — inequality and attack vectors analysis

Building our early work on mev in eth2, we are looking to model further the inequalities that may be caused by MEV as well as study potential vectors of attack of eth2 related to MEV. In particular we are looking to answer: 1) to what extent does MEV in eth2 amplify its inherent rich-get-richer dynamics?, 2) how does knowing the block proposers in advance change MEV extraction dynamics?

- Flashbots in eth2

After an initial exploration of MEV in eth2 and the Rayonism hackathon where a spec of an eth1+eth2 MEV client was built out, we dive deeper into specing out Flashbots in eth2. This includes thinking about the best flow for MEV rewards to be distributed, understanding different validator pool architectures and ensuring MEV extraction is available to validators of all sizes.

- MEV in L2s

MEV will likely exist in each L2s being deployed as well as across them. This effort aims to start doing research on the topic, both on how MEV exists at these layers and the state of its mitigation via different solutions such as VDFs and fair ordering protocols.

- MEV after EIP-1559

EIP-1559 is a hotly debated upcoming EIP that is being introduced in the London Hardfork. It will significantly alter Ethereum's fee mechanism, crucially resulting in most of the transaction fee being burned and eliminating 0 gas price transactions. We examine the effects of EIP-1559 on MEV extraction and, by extension, the Flashbots project.

- Cryptoeconomic design exploration

We explore whether there are cryptoeconomic mechanisms that can reinforce, or substitute the relatively expensive and proprietary solution that is SGX, to achieve the same desirable result of complete pre-trade privacy. Some work already published includes thoughts shared by Vitalik Buterin in an [EthResearch post](#) for a fee market design where block proposers and block builders are separate entities.

- Mempool privacy

A survey of privacy solutions that can be used to provide MEV-Geth with mempool privacy and an attempt to start formalizing the problem of mempool privacy for L1 and L2 blockchain constructions.

- Auction mechanisms survey

An investigation and survey of the existing literature of auction mechanism design to motivate the design of the block space and transaction ordering auctions enabled by mev-geth. The high-level research question is: What is a good auction mechanism for mev-geth auctions?

Community

MEV.wtf Summit

Join our full-day [MEV.wtf](#) summit with ETHGlobal on Thursday, Jul 1, where we will discuss the core problems of MEV, mitigations and solutions from the application-agnostic protocol level and application-specific level.

ETHGlobal HackMoney hackathon

Jam with us at the ETHGlobal HackMoney hackathon (Jun 18 — Jul 9, 2021) where Flashbots is providing \$8,000 in prizes to winning hacks built around MEV. Additionally, we are giving out \$4,000 in joint prizes with Uniswap for a series of ideas built on both Uniswap and Flashbots during the hackathon.

ArcherSwap's Trader Extractable Value

ArcherDAO has built a DEX which sends users' Uniswap and Sushiswap transactions directly to miners as Flashbots bundles, thereby skipping the mempool where hungry sandwich bots are watching. Moreover, doing so also allows users to avoid paying for failed transactions.

Some trades through Archerswap create arbitrage opportunities, and Archer released an update to their DEX where they have started to backrun their users to capture these and kick them back to the trader. That way the trader gets better pricing and captures some amount of the MEV they create. We think this is the start of a long list of protocols which will use MEV in creative ways to offer better outcomes for their users.

1inch offers private transactions through Flashbots

<https://help.1inch.io/en/articles/5300755-what-are-flashbot-transactions-and-how-do-they-work-on-1inch>

1inch, one of the largest DEXes in Ethereum, now offers the ability for customers to send their transactions via Flashbots bundles, thus offering frontrunning protection from the monsters of the mempool.

mistX launches a gasless DEX

mistX is a DEX that offers users the interesting new feature of allowing the trader to not pay a transaction fee to the miner. Instead the trader pays the miner via a smart contract call in mistX's smart contract, and mistX will either remove some ETH from the trade or from the user's wallet to pay this fee.

Similar to 1inch or ArcherSwap, mistX also offers frontrunning protection and no failed transactions to their users. Hasu of Paradigm published a great article on mistX [here](#).

Flashbots on Bloomberg

Flashbots had our first mention in the mainstream media! Check out this clip at [1:30](#) to see it for yourself.

Flashbots Bundle Explorer

The community built [Flashbots Bundle Explorer](#), maintained by [martriay](#), keeps adding new features, now supporting multiple bundles and displaying the assets touched in each transaction as well.

Get involved

At Flashbots, we research and build systems around MEV, and we would love to collaborate with you. We are a distributed organization with the principles of a [pirate hacker collective](#), and have several [open positions](#). We also issue grants to external researchers doing work aligned with ours, please find out more in our [Research repository](#), or join our [Discord](#)!